

On the Role of Shared Entanglement

Dmitry Gavinsky

Department of Computer Science

University of Calgary

Calgary, Alberta, Canada, T2N 1N4

Abstract

Despite the apparent similarity between shared randomness and shared entanglement in the context of Communication Complexity, our understanding of the latter is not as good as of the former. In particular, there is no known “entanglement analogue” for the famous theorem by Newman, saying that the number of shared random bits required for solving any communication problem can be at most logarithmic in the input length (i.e., using more than $O(\log n)$ shared random bits would not reduce the complexity of an optimal solution).

In this paper we prove that the same is not true for entanglement. We establish a wide range of tight (up to a polylogarithmic factor) entanglement vs. communication tradeoffs for relational problems. The low end is: for any $t > 2$, reducing shared entanglement from $\log^t n$ to $o(\log^{t-2} n)$ qubits can increase the communication required for solving a problem almost exponentially, from $O(\log^t n)$ to $\Omega(\sqrt{n})$. The high end is: for any $\varepsilon > 0$, reducing shared entanglement from $n^{1-\varepsilon} \log n$ to $o(n^{1-\varepsilon}/\log n)$ can increase the required communication from $O(n^{1-\varepsilon} \log n)$ to $\Omega(n^{1-\varepsilon/2}/\log n)$. The upper bounds are demonstrated via protocols which are *exact* and work in the *simultaneous message passing model*, while the lower bounds hold for *bounded-error protocols*, even in the more powerful *model of 1-way communication*. Our protocols use shared EPR pairs while the lower bounds apply to any sort of prior entanglement.

We base the lower bounds on a strong direct product theorem for communication complexity of a certain class of relational problems. We believe that the theorem might have applications outside the scope of this work.

1 Introduction

Suppose that Alice, Bob and Charlie play the following game: Alice receives an n -bit binary string x , Bob receives a string y of the same length, they both send some information to Charlie, who then tries to guess (based on the received messages) whether $x = y$ or not. The goal is for Alice and Bob to send as short messages as possible, such that Charlie would still be able to answer correctly with probability at least $3/4$. Assume that before the game starts Alice and Bob choose two random binary strings r_1 and r_2 , of length 2^n each. Then they treat their n -bit inputs as indices in the range $[1..2^n]$ and send to Charlie the bits which are on the positions x and y of r_1 and r_2 (i.e., Alice and Bob send 2 bits each). Eventually, Charlie decides that $x = y$ if the pairs of bits received from Alice and Bob are the same, otherwise he declares that $x \neq y$. It is clear that if Charlie guesses that $x = y$ then he is correct with probability $3/4$ and if he says that $x \neq y$ then he is certainly right. So, we see that the problem can be solved by communicating only 4 bits (for any input length n). On the other hand, Newman and Szegedy [NS96] have shown that if Alice and Bob do not share random bits then they must communicate at least $\Omega(\sqrt{n})$ bits in order to win the game with any constant probability greater than $1/2$.

We can let our players use the laws of quantum mechanics in order to further increase their strength. Specifically, they can share *entanglement*.¹ In this case they are allowed to apply any quantum-mechanical operation to their subspaces of the common Hilbert space. In particular, they can perform measurements and their behavior may depend on the outcomes of the measurements.

If the players share a sequence of random bits (chosen uniformly and independently) we say that they are using *shared* or *public randomness* (also called a *public coin*). If the players share a quantum state we say that they are using *shared entanglement* (note that it would be useless to share a state which is not entangled w.r.t. the players' local subspaces). It is easy to see that in the model of shared entanglement the players are at least as strong as they are in the model of shared randomness (k independent shared EPR pairs can be measured locally in order to get k perfect random bits).

In this paper we will deal with a longstanding open question regarding the power of quantum entanglement in communication.

1.1 Shared randomness and shared entanglement

Let us generalize our framework, suppose that Alice and Bob have to fulfill some computation-flavored distributed task. As before, the players are located far from one another, so that communication between them is expensive or even impossible. The players are all powerful from the computational aspect.

Two well known instances of this framework are 2-prover proof systems and various models of 2-party communication complexity.

In the first case Alice and Bob are provers, they can communicate with a *verifier* but not with one another. The verifier is computationally limited. The goal of the provers is to convince the verifier that some string x belongs to a language L , when checking validity of that statement is beyond the verifier's computational ability. If the verifier believes, based on its communication with the provers, that $x \in L$ then we say that x is *accepted*, otherwise it is *rejected*. A language L has a *valid 2-prover proof system* if Alice and Bob can make the verifier accept (with high probability) any $x \in L$, but making it to accept some $y \notin L$ would be (almost) impossible.

¹Note that even if Alice and Bob share a quantum state the communication channels are still assumed to be classical. For simplicity in this paper we do not deal with quantum communication, even though it seems that some of our results generalize to that case.

In the models of 2-party communication complexity Alice and Bob receive one piece of input each, respectively denoted by x and y . In the strongest considered model communication between Alice and Bob is possible but expensive, it goes in many rounds (first Alice sends a message to Bob, then Bob replies, then Alice sends another message and so on). Their goal is to compute (with high probability) some function $f(x, y)$ using the smallest possible amount of communication.

One possible restriction of the model is *1-way communication*: Alice is permitted to send a message to Bob, after that he has to produce an output (based on y and the message from Alice). Note that unlike the unrestricted case, the 1-way model is not symmetric w.r.t. x and y . Sometimes even more restricted (symmetric) case is considered which has been described in the beginning: there is another participant called a *referee*, Alice and Bob can send one message each to the referee and it has to produce an output based on those two messages. This model is called *simultaneous message passing (SMP)*, it is arguably the weakest setting of 2-party communication complexity that is still interesting.

A *communication protocol* is a description of the behavior of all the participants. The *communication cost* of a protocol is the maximum possible total length of the messages sent according to the protocol till the output is produced. The optimization problem is to find a least expensive protocol which enables the players to solve their task; the *communication cost* of a communication task is the cost of an optimal protocol.

Sometimes the communication task is defined not as a function but rather as a *relational problem*. In that case for a pair (x, y) in the input there can be defined any number of good answers (no good answer means that the pair can never be given as input). In this paper we allow this more general form of communication problems.

In all these models (both 2-prover proof systems and 2-party communication complexity settings) we understand relatively well what the power of shared randomness is. In the case of proof systems two classical all-powerful provers can prove to a polynomially-bounded verifier² membership in L if and only if $L \in NEXP$ ([BFL90], [R95]). It is also known that shared randomness does not affect the power of a system ([GS86]).

In the case of 2-party communication complexity the situation is slightly more complicated. It has been demonstrated by Newman [N91] that we can assume without loss of generality that the number of shared random bits used by a protocol is at most logarithmic in the input length. Therefore, availability of shared randomness cannot reduce significantly the complexity in the models where Alice sends at least one message to Bob (she can append the required number of randomly chosen bits to her message, that would increase the cost of a protocol only by an additive logarithmic term). In the case of SMP the presence of shared randomness can make a difference. For instance, as mentioned in the beginning, the *equality problem* can be solved by a protocol of constant cost when shared randomness is available, whereas without shared randomness the complexity becomes $\Omega(\sqrt{n})$ ([NS96]).

We know much less about the role of shared entanglement in the context of these models. We do not know what the power of 2-prover proof systems is when the provers share entanglement.³ Moreover, Cleve, Høyer, Toner and Watrous [CHTW04] have shown that the known protocol which accepts $NEXP$ in the standard 2-prover system cannot achieve the same goal in the presence of shared entanglement, unless $EXP = NEXP$. For the restricted case when the provers share only polynomial (in n) number of qubits, it has been demonstrated by Kobayashi and Matsumoto [KM03] that only languages from $NEXP$ can be accepted (but again, maybe not all of them).

²In particular, that means that the communication cost of a proof can be at most polynomial in the input length.

³As far as we know today, such systems can be more powerful, less powerful, or even incomparable to the standard 2-prover systems, since adding power to provers can, in general, help them to establish a true argument as well as to cheat.

In the area of communication complexity very recently a communication task has been found ([GKRW06]) which can be solved exponentially more efficiently in the SMP model with shared entanglement than in the SMP model with shared randomness (in fact, the problem is equally hard even for 1-way communication with shared randomness). But it is not known whether any upper bound can be put on the number of qubits in a potentially helpful shared quantum state.

There is a result by Shi [S05] which says (informally) that adding large amounts of prior entanglement can reduce the communication no more than exponentially. However, Jain, Radhakrishnan and Sen [JRS05] have shown that Newman’s “blackbox-type” proof, which keeps the protocol the same and just reduces the set of random strings to $O(n)$ elements (which in turn can be represented by $O(\log n)$ random bits), cannot be used in order to reduce the amount of entanglement used.

Besides, it is not clear whether EPR pairs can be considered as a universal source of entanglement in the contexts of 2-prover proof systems and 2-party communication complexity.

1.2 Our results

As our main result, we claim that no reasonably sublinear upper bound holds for the number of potentially useful shared entangled qubits. Put in contrast to the Newman’s theorem, this is a new example of qualitative difference between the two resources (public coin vs. shared entanglement). Note that our conclusion and that of [GKRW06] are logically related, our result can be viewed as a generalization of the models separation in [GKRW06].⁴

Formally, our main result is the following.

Theorem 1. *For any monotone increasing function $k(\cdot) : \mathbb{N} \rightarrow \mathbb{N}$ there exists a family of relational communication problems such that the problem with input length $n = m \cdot k(m)$ can be solved exactly in the SMP model with $k(m) \log(m)$ shared EPR pairs by a protocol of cost $O(k(m) \log(m))$. The same problem requires $\Omega\left(\frac{k(m)\sqrt{m}}{\log m}\right)$ communication for its solution with constant-bounded error in the model of 1-way communication with any shared entangled state of $o\left(\frac{k(m)}{\log m}\right)$ qubits.*

In particular, for any $t > 2$ by choosing $k(m) = \log^{t-1} m$ we obtain a problem with input length $n = m \cdot \log^{t-1} m$ which can be solved using (less than) $\log^t n$ EPR pairs and $O(\log^t n)$ communication but requires $\Omega(\sqrt{n})$ communication with $o(\log^{t-2} n)$ shared entanglement. Therefore, limiting the amount of shared entanglement even to super-logarithmic values can result in almost exponential increase in communication cost of a problem.

Alternatively, for any $\varepsilon > 0$ choosing $k(m) = m^{1/\varepsilon-1}$ gives a problem with input length $n = m^{1/\varepsilon}$, solvable with (less than) $n^{1-\varepsilon} \log n$ EPR pairs and $O(n^{1-\varepsilon} \log n)$ communication but demanding $\Omega\left(\frac{n^{1-\varepsilon/2}}{\log n}\right)$ communication with $o\left(\frac{n^{1-\varepsilon}}{\log n}\right)$ entanglement. Therefore, no reasonably sublinear upper bound on the number of useful shared qubits can be put.

Note that our protocols use shared EPR pairs whereas the lower bounds hold for any sort of entanglement. Because our analysis is tight up to a polylogarithmic factor, it can be concluded that for the families of relations we consider it is the case that independent EPR pairs are as good as any sort of shared entanglement can be (up to a polylogarithmic factor). Our protocols are exact and work in the SMP model, while the lower bounds hold for bounded-error protocols, even in the model of 1-way communication.

⁴Assume towards contradiction that shared entanglement is no more powerful than public randomness (this is a contrapositive to [GKRW06]). Then any number of shared qubits can be replaced by similar number of public random bits, which can be reduced to logarithmic number (due to Newman) and then simulated by the same number of shared EPR pairs. So, logarithmic number of shared EPR pairs would always be sufficient, which is a contrapositive to our main statement.

Our proof consists of two parts. First, we establish a strong direct product theorem for a class of relational problems in the model of 1-way communication.⁵ In particular, the theorem is applicable to the relation *HMP* defined by Bar-Yossef, Jayram and Kerenidis [BJK04]. We think that the theorem might be of independent interest. For instance, the fact that it gives a strong direct product result for the one-way complexity of *HMP* looks very promising, because this relation, and its modifications, is the only known type of communication problem that demonstrates superpolynomial separation between quantum and classical 1-way models. Problems based on *HMP* have been used recently to establish a number of exponential separations between various quantum and classical communication models (cf. [BJK04], [GKRW06]). It might be the case that our strong direct product result can be used to obtain more results based on *HMP*.

The second part is a construction of an entanglement-expensive communication task. We first apply our direct product theorem in order to reduce to exponentially low the maximum success probability of a protocol which is not using entanglement. Then we view a hypothetical protocol which is successful when it uses a shared entangled state ρ as a distinguisher between ρ and the maximally mixed state of the same dimension. If the protocol starts with the maximally mixed shared state then the players are *not entangled*, so the upper bound on success probability without entanglement must hold. By the laws of quantum mechanics, any distinguisher between ρ and the maximally mixed state must be wrong with probability not less than approximately the inverse of the dimension of the state. So, our assumption that a protocol starting with ρ is successful leads to a lower bound on the dimension of ρ (in our case the obtained bounds are tight up to a polylogarithmic factor in terms of the *number of qubits* in ρ). Note that the resulting entanglement lower bound itself has the form of a direct product result (i.e., in order to solve more copies of the original problem one must accordingly increase the number of shared entangled qubits to start with).

It can be seen that the described technique is quite general; probably it can be used in other situations where the “entanglement complexity” of a problem is considered (including all the models we have mentioned). For instance, given a corresponding direct product result for the complexity of a solution without entanglement, the technique can be applied to virtually any communication complexity model.

We note that the technique of replacing a quantum state under consideration by the maximally mixed state and upper-bounding the damage caused by such substitution has been used before in several contexts related to communication complexity (cf. [KSW04], [A04]). It seems that the technique is quite powerful and might be applicable in various settings involving quantum mechanics and information processing.

We also apply our entanglement bounding idea in the context of 2-prover proof systems. We give a partial converse to the result of [KM03]. We characterize the power of 2-prover proof systems, where the provers are allowed to share entanglement but the number of qubits is bounded by a polynomial *fixed a priori* (i.e., the bound should be a global parameter of the model).⁶ The power of such proof systems equals *NEXP*, i.e., in this case the factor of entanglement does not affect the power of a system.

⁵We call a direct product result *strong* if the amount of available resources scales up as the number of instances grows.

⁶Note that the model considered by [KM03] gives the provers more freedom than we do. Their provers can use the amount of entanglement which is bounded *per protocol*, while ours are bounded *per model*. It is still open whether the proof system of [KM03] can accept any language in *NEXP*.

2 Preliminaries

In this paper we will deal with relational communication problems. Formally, a problem will be represented as $P \subseteq X \times Y \times Z$, where $X = Y = \{0,1\}^*$ are the sets of inputs to Alice and Bob, correspondingly, and Z is the set of possible answers. An answer $z \in Z$ is good for input $(x, y) \in X \times Y$ if $(x, y, z) \in P$; if no such z exists then the combination (x, y) is forbidden (i.e., it is never given as input). We will write X_n to denote $X \cap \{0,1\}^n$ as well as Y_n and Z_n to denote $\{y \in Y \mid \exists x \in X_n, z \in Z : (x, y, z) \in P\}$ and $\{z \in Z \mid \exists x \in X_n, y \in Y : (x, y, z) \in P\}$, correspondingly.

Let $P \subseteq X \times Y \times Z$ be a relational problem. When P is clear from the context, for any $A \subseteq X$, $y \in Y$ and $z \in Z$ we will denote by $A_{|y,z}$ the set $\{x \in A \mid (x, y, z) \in P\}$.

We write $P^k \subseteq X^k \times Y^k \times Z^k$ to address the direct product of k instances of P , formally:

$$P^k = \{((x_1, \dots, x_k), (y_1, \dots, y_k), (z_1, \dots, z_k)) \mid \forall i \in \{1, \dots, k\} : (x_i, y_i, z_i) \in P\},$$

in that case we will address P as a *single instance* of a problem. For any $A \subseteq X^k$, $i \leq k$, $a_1, \dots, a_i \in Y$ and $b_1, \dots, b_i \in Z$ we define:

$$A_{|a_1, \dots, a_i, b_1, \dots, b_i} \stackrel{\text{def}}{=} \{x \in A \mid \forall 1 \leq j \leq i : (x_j, a_j, b_j) \in P\},$$

and for $a \in Y$ and $b \in Z$:

$$A_{|y_i=a, z_i=b} \stackrel{\text{def}}{=} \{x \in A \mid (x_i, a, b) \in P\}.$$

Note that in our definitions of k -ary direct products we have changed the natural ordering and grouping of elements, making them more suitable for our context of communication tasks.

For convenience we assume that 1-way protocols do not use shared randomness (private random bits will be allowed, of course). As explained earlier, this does not cause any loss of generality because that assumption can, in the worst case, result in adding a logarithmic factor to the communication cost.

For any discrete set A we denote by \mathcal{U}_A the uniform distribution over A . For a discrete random variable x we denote by $\mathbf{H}[x]$ its Shannon entropy. Sometimes we write $\mathbf{H}_D[x]$ for a distribution D to emphasize that $x \sim D$, the same value will be denoted by $\mathbf{H}[D]$ when x is insignificant for the context.

We write \log to denote the logarithmic function with base 2.

3 A strong direct product theorem for relations

We establish a strong direct product theorem for a class of relational problems in the model of 1-way communication without shared entanglement.

Lemma 2. *Let $P \subseteq X \times Y \times Z$ be a relation. Let $\sigma(m) : \mathbb{N} \rightarrow \mathbb{R}$ and $\delta(m) : \mathbb{N} \rightarrow [0, 1]$ be two functions, such that $\log m \leq \sigma(m) \leq m$, $\log\left(\frac{1}{\delta(m)}\right) \geq 4 + 6\frac{\log(|Z_m|)}{\log m}$ and for any distribution D over X_m with $\mathbf{H}_D[x] \geq m - \sigma(m)$ it holds that*

$$\Pr_{(y,z) \sim \mathcal{U}_{Y \times Z}} \left[\Pr_{x \sim D} [(x, y, z) \in P] \geq \frac{2}{3} \right] \leq \frac{\delta(m)}{|Z_m|}.$$

Then for $m \geq 64$ and $k \geq \log m$, for any set $B \subseteq (X_m)^k$ of size at least $2^{km - \frac{k\sigma(m)}{\log m}}$ the following holds:

$$\Pr_{y \sim \mathcal{U}_{Y^k}} \left[\exists z \in Z^k : |B_{|y,z}| \geq (2/3)^{\frac{k}{\log m}} |B| \right] \leq 2^{-k}.$$

Proof of Lemma 2. Fix a set B satisfying the lemma condition. Define:

$$\mathcal{E}(y, z) \stackrel{\text{def}}{=} \begin{cases} 1 & \text{if } |B_{|y, z}| \geq (2/3)^{\frac{k}{\log m}} |B|, \\ 0 & \text{otherwise} \end{cases},$$

and we will use the same notation for the corresponding logical predicate (i.e., $\mathcal{E}(y, z)$ is satisfied if and only if $\mathcal{E}(y, z) = 1$). It holds that

$$\Pr_{y \sim \mathcal{U}_{Y^k}} [\exists z \in Z^k : \mathcal{E}(y, z)] \leq \mathbf{E}_{y \sim \mathcal{U}_{Y^k}} \left[\sum_{z \in Z^k} \mathcal{E}(y, z) \right] = |Z^k| \cdot \Pr_{(y, z) \sim \mathcal{U}_{Y^k \times Z^k}} [\mathcal{E}(y, z)].$$

We will upper-bound the expression on the right-hand side. Before we proceed, let us introduce some notation. We will address individual coordinates of elements of X^k , Y^k and Z^k through (x_1, \dots, x_k) for an $x \in X^k$, and similarly for $y \in Y^k$ and $z \in Z^k$.

Let us think of choosing $(y, z) \sim \mathcal{U}_{Y^k \times Z^k}$ as a sequential k -step process of choosing pairs $(y_i, z_i) \sim \mathcal{U}_{Y \times Z}$, not necessarily in the ascending order of i -s. We will specify the order later, so far we denote it by j_1, \dots, j_k , i.e., at the first step we choose (y_{j_1}, z_{j_1}) , and so on.

Let a_{j_1}, \dots, a_{j_k} and b_{j_1}, \dots, b_{j_k} be the choices made for the random variables y_{j_1}, \dots, y_{j_k} and z_{j_1}, \dots, z_{j_k} , correspondingly. Define: $B_0 \stackrel{\text{def}}{=} B$ and for $1 \leq i \leq k$: $B_i \stackrel{\text{def}}{=} B_{i-1}|_{y_{j_i}=a_{j_i}, z_{j_i}=b_{j_i}}$.

Consider the sequence $|B_0|, \dots, |B_k|$ – it is monotone non-increasing, and $\mathcal{E}(y, z)$ exactly means that $|B_k| \geq (2/3)^{k/\log m} |B|$. Let us say that step i is *good* if $|B_i| / |B_{i-1}| \geq 2/3$. Observe that $\mathcal{E}(y, z)$ occurs only if at least $k - \frac{k}{\log m}$ steps were good. Assuming integer-valued rounding where necessary, we get

$$\Pr[\mathcal{E}(y, z)] \leq \Pr \left[\text{at least } k - \frac{k}{\log m} \text{ steps were good} \right] \leq \binom{k}{k - \frac{k}{\log m}} \cdot \max_{i_1, \dots, i_{k - \frac{k}{\log m}}} \left\{ \Pr \left[\text{the steps } i_1, \dots, i_{k - \frac{k}{\log m}} \text{ were good} \right] \right\},$$

where the maximum is taken over all $(k - \frac{k}{\log m})$ -tuples of pairwise distinct indices from $[k]$. For the reasons which will become clear later, we do not want to take into consideration the last $\frac{2k}{\log m}$ steps, so we let those steps be good “for free” and get

$$\Pr[\mathcal{E}(y, z)] \leq \binom{k}{k - \frac{k}{\log m}} \cdot \max_{i_1, \dots, i_{k - \frac{3k}{\log m}}} \left\{ \Pr \left[\text{the steps } i_1, \dots, i_{k - \frac{3k}{\log m}} \text{ were good} \right] \right\} \leq 2^k \cdot \left(\max_{i \in [k - \frac{2k}{\log m}]} \left\{ \Pr[\text{the } i \text{ 'th step was good}] \right\} \right)^{k - \frac{3k}{\log m}},$$

where the first maximum is taken over all $(k - \frac{3k}{\log m})$ -tuples of pairwise distinct indices from $[k - \frac{2k}{\log m}]$. We can make our bound tighter using the fact that the event $\mathcal{E}(y, z)$ implies that all B_i -s are of size at least $(2/3)^{k/\log m} |B| \geq 2^{km - \frac{k\sigma(m)}{\log m} - k}$:

$$\Pr[\mathcal{E}(y, z)] \leq 2^k \cdot \left(\max_{i \in [k - \frac{2k}{\log m}]} \left\{ \Pr \left[\text{the } i \text{ 'th step was good} \mid |B_{i-1}| \geq 2^{km - \frac{k\sigma(m)}{\log m} - k} \right] \right\} \right)^{k - \frac{3k}{\log m}}.$$

Denote:

$$p_{max} \stackrel{\text{def}}{=} \max_{i \in [k - \frac{2k}{\log m}]} \left\{ \Pr \left[\text{the } i \text{ 'th step was good} \mid |B_{i-1}| \geq 2^{km - \frac{k\sigma(m)}{\log m} - k} \right] \right\}.$$

We have seen that

$$\Pr_{y \sim \mathcal{U}_{Y^k}} \left[\exists z \in Z^k : \mathcal{E}(y, z) \right] \leq |Z_m|^k \cdot 2^k \cdot p_{max}^{k - \frac{3k}{\log m}}. \quad (1)$$

For obtaining the desired bound we will, on each step, try to choose a coordinate which has low chances to give rise to a good step. Such a coordinate for the i 'th step will be chosen adaptively among all those not fixed in the first $i - 1$ steps.

Assume that we are at step i_0 now, let us see that such a bad coordinate must exist as long as $|B_{i_0-1}| \geq 2^{km - \frac{k\sigma(m)}{\log m} - k}$ and $i_0 \leq k - \frac{2k}{\log m}$. Let D_{i_0-1} be the uniform distribution over B_{i_0-1} , we know that $\mathbf{H}_{D_{i_0-1}}[x] \geq km - \frac{k\sigma(m)}{\log m} - k$. For $j \in [k]$ define e_j to be the entropy of x_j when $x \sim D_{i_0-1}$ and let $J \stackrel{\text{def}}{=} \{e_j \geq m - \sigma(m) \mid j \in [k]\}$. Because $\forall j \in [k] : e_j \leq m$, by the pigeonhole principle and entropy subadditivity it must hold that

$$\begin{aligned} |J|m + (k - |J|)(m - \sigma(m)) &\geq km - \frac{k\sigma(m)}{\log m} - k \\ k - |J| &\leq \frac{k}{\log m} + \frac{k}{\sigma(m)} \leq \frac{2k}{\log m} \\ |J| &\geq k - \frac{2k}{\log m}. \end{aligned}$$

Choose arbitrary $j_0 \in J$, such that y_{j_0} and z_{j_0} have not been set yet (it exists because we are only at step $i_0 \leq k - \frac{2k}{\log m}$).

Observe that

$$\Pr_{(a,b) \sim \mathcal{U}_{Y \times Z}} \left[\left| B_{i_0-1} \mid_{y_{j_0}=a, z_{j_0}=b} \right| \geq \frac{2}{3} |B_{i_0-1}| \right] \leq \frac{\delta(m)}{|Z_m|},$$

by the theorem assumption about P applied to the j_0 'th coordinate of P^k . So we choose j_0 as the coordinate to be handled at step i_0 . Because $B_i = B_{i-1} \mid_{y_{j_0}=a, z_{j_0}=b}$, where $(a,b) \sim \mathcal{U}_{Y \times Z}$, we conclude that the probability of i 'th step to be good is at most $\delta(m)/|Z_m|$.

Recall that our goal is to upper-bound the value of p_{max} . We have chosen i_0 to be any integer not exceeding $k - \frac{2k}{\log m}$, so an upper bound on \Pr [the i_0 'th step was good] under our assumptions is also an upper bound on p_{max} . Therefore, (1) leads to the required

$$\Pr_{y \sim \mathcal{U}_{Y^k}} \left[\exists z \in Z^k : \mathcal{E}(y, z) \right] \leq |Z_m|^k \cdot 2^k \cdot \left(\frac{\delta(m)}{|Z_m|} \right)^{k - \frac{3k}{\log m}} \leq |Z_m|^{\frac{3k}{\log m}} \cdot 2^k \cdot (\delta(m))^{k - \frac{3k}{\log m}} \leq 2^{-k},$$

where the last inequality follows from the theorem assumptions regarding $\delta(\cdot)$ and m . ■ *Lemma 2*

The following theorem is straightforward from Lemma 2:

Theorem 3. *Let $P \subseteq X \times Y \times Z$ be a relation satisfying the condition of Lemma 2.*

Then for m large enough and $k \geq \log m$, any 1-way communication protocol of complexity at most $\frac{k\sigma(m)}{\log m} - 2$ solves P^k with success probability at most $(2/3)^{\frac{k}{\log m} - 2}$.

Proof of Theorem 3. Assume towards contradiction that there exists a protocol A of complexity at most $\frac{k\sigma(m)}{\log m} - 2$ which solves P^k with success probability more than $(2/3)^{\frac{k}{\log m} - 2}$. Then there exists a deterministic protocol A' which does the same when the input distribution is $\mathcal{U}_{X^k \times Y^k}$.

Assume that $x \sim \mathcal{U}_{X^k}$ and $y \sim \mathcal{U}_{Y^k}$. For any message ever sent by Alice according to A' , define its *weight* as the probability of the message to be produced and its *success* as the probability that A' is successful, conditioned on the message having been produced. By the pigeonhole principle, with probability at least $3/4$ Alice sends a message of weight at least $1/4$ divided by the number of possible messages. Similarly, with probability at least $1/3$ Alice sends a message of success at least $2/3$ times the success probability of the protocol. In other words, there exists some message α such that

$$B \stackrel{\text{def}}{=} \left\{ x \in X^k \mid \text{given } x, \text{ Alice sends } \alpha \text{ according to } A' \right\}$$

satisfies $|B| \geq 2^{\frac{k\sigma(m)}{\log m}}$, and conditioned on Alice sending α , Bob is able to produce a correct answer with probability more than $(2/3)^{\frac{k}{\log m} - 1}$.

Let $z(y)$ be defined as the answer produced by Bob according to A' , if his own input is y and the message received from Alice is α . Then, according to the previous discussion, it must hold that

$$\Pr_{(x,y) \sim \mathcal{U}_{B \times Y^k}} \left[(x, y, z(y)) \in P^k \right] > (2/3)^{\frac{k}{\log m} - 1},$$

which leads to

$$\Pr_{y \sim \mathcal{U}_{Y^k}} \left[\Pr_{x \sim \mathcal{U}_B} \left[(x, y, z(y)) \in P^k \right] > (2/3)^{\frac{k}{\log m}} \right] > (2/3)^{\frac{k}{\log m}}.$$

In other words,

$$\Pr_{y \sim \mathcal{U}_{Y^k}} \left[|B_{y, z(y)}| \geq (2/3)^{\frac{k}{\log m}} |B| \right] > (2/3)^{\frac{k}{\log m}},$$

which contradicts Lemma 2.

Our theorem follows. ■ *Theorem 3*

4 A communication task with an entanglement-expensive solution

Let m be a power of 2. The following relational problem has been first studied by Bar-Yossef, Jayram and Kerenidis [BJK04].

Definition 1. Let $X = \{0, 1\}^m$, and let M_m be the family of all perfect matchings on m nodes, represented as $m/2$ -tuples of pairs of vertices connected by an edge. Then

$$HMP_m = \left\{ (x, y, (a, x_i \oplus x_j)) \mid x \in X, y \in M_m, y_a = \{i, j\} \right\}.$$

In words, Alice receives a binary coloring of m nodes and Bob receives a perfect matching on m nodes; the goal is to say whether a pair of nodes connected by the matchings are colored the same or not.

Let k be an integer greater than 1. We define $HMP_m^{(k)}$ as a direct product of k instances of HMP_m .

Definition 2. $HMP_m^{(k)} = \left\{ ((x_1, \dots, x_k), (y_1, \dots, y_k), (z_1, \dots, z_k)) \right\}$, where for all $i \in \{1, \dots, k\}$ it holds that $(x_i, y_i, z_i) \in HMP_m$.

We will consider the communication complexity of certain sub-families of $HMP_m^{(k)}$ in order to establish our entanglement vs. communication tradeoffs.

4.1 Complexity of HMP_m

It is known that HMP_m can be solved exactly using $\log(m)$ EPR pairs and $O(\log(m))$ bits of communication in the SMP model. The protocol is a modification of a construction suggested by Buhrman [B] (a similar protocol is used in [GKRW06]). For completeness we describe the protocol here.

The starting state of Alice and Bob is

$$\frac{1}{\sqrt{m}} \sum_{i \in \{0,1\}^{\log m}} |i\rangle |i\rangle.$$

First, Alice applies phases according to her input x :

$$\frac{1}{\sqrt{m}} \sum_{i \in \{0,1\}^{\log m}} (-1)^{x_i} |i\rangle |i\rangle$$

and Bob measures with the $m/2$ projectors $E_{i,j} = |i\rangle\langle i| + |j\rangle\langle j|$ induced by the pairs $\{i, j\} \in y$. After that both players apply a Hadamard transform to each of the $\log n$ qubits of their part of the shared state, which then becomes (ignoring normalization)

$$\sum_{k,l} \left((-1)^{x_i + (k \oplus l) \cdot i} + (-1)^{x_j + (k \oplus l) \cdot j} \right) |k\rangle |l\rangle,$$

where $\{i, j\}$ is the outcome of the Bob's measurement, \oplus denotes the bit-wise xor operation and \cdot stands for the inner product *mod 2* of two vectors. It follows that $|k\rangle |l\rangle$ has non-zero amplitude if and only if

$$(k \oplus l) \cdot (i \oplus j) = x_i \oplus x_j.$$

The players measure the state $|k\rangle |l\rangle$ in the computational basis, then Alice sends k and Bob sends a, i, j and l to the referee, where $y_a = \{i, j\}$. The referee outputs $(a, (k \oplus l) \cdot (i \oplus j))$, and the protocol is always correct.

Concerning the lower bound, it has been demonstrated in [BJK04] that HMP_m is hard for 1-way communication without entanglement. However, we need a stronger statement, in order to be able to apply Theorem 3.

Claim 4. Let $\sigma(m) = \frac{\sqrt{m-1}}{576}$ and $\delta = \frac{1}{2^{10}}$, then for any distribution D over X_m with $\mathbf{H}_D[x] \geq m - \sigma(m)$ it holds that

$$\Pr_{(y,z) \sim \mathcal{U}_{Y \times Z}} \left[\Pr_{x \sim D} [(x, y, z) \in HMP_m] \geq \frac{2}{3} \right] \leq \frac{\delta}{m}.$$

Proof of Claim 4. Assume towards contradiction that that exists some distribution D_0 which falsifies the claim.

Corresponding to the statement of the claim is the process of choosing $y \sim \mathcal{U}_{M_m}$ and $z = (a, b)$, where $a \sim \mathcal{U}_{[m/2]}$ and $b \sim \mathcal{U}_{\{0,1\}}$. The choice is followed by asking what $\Pr[(x, y, z) \in HMP_m]$ is w.r.t. $x \sim D$. This is equivalent to uniformly choosing two endpoints $i \neq j \in [m]$ and $b \in \{0, 1\}$, followed by asking what the probability is that $x_i \oplus x_j = b$ w.r.t. $x \sim D$. Our assumption can be rephrased as

$$\Pr_{i \neq j \sim \mathcal{U}_{[m]}; b \sim \mathcal{U}_{\{0,1\}}} \left[\Pr_{x \sim D_0} [x_i \oplus x_j = b] \geq \frac{2}{3} \right] > \frac{\delta}{m}. \quad (2)$$

Define:

$$C = \left\{ \{i, j\} \mid i \neq j \in [m]; \exists b \in \{0, 1\} : \mathbf{Pr}_{x \sim D_0} [x_i \oplus x_j = b] \geq 2/3 \right\}.$$

Since it cannot hold for any $i \neq j$ that both $x_i \oplus x_j = 0$ and $x_i \oplus x_j = 1$ occur with probability at least $2/3$, it follows from (2) that $|C| \geq \frac{\delta}{m}(m^2 - m) = \delta(m - 1)$.

Now consider the graph consisting of the edges from C . This graph must contain at least $\sqrt{2|C|}$ non-isolated vertices, since v vertices give only $(v^2 - v)/2 < v^2/2$ distinct edges. Let $C' \subseteq C$ be a forest consisting of a spanning tree for each connected component of this graph. It must hold that $|C'| \geq \sqrt{|C|/2} \geq \sqrt{(m - 1)\delta/2}$.

Note that the set of uniformly distributed binary random variables $\{x_i \oplus x_j \mid \{i, j\} \in C'\}$ is perfectly independent when $x \sim \mathcal{U}_{\{0,1\}^m}$. Therefore by entropy subadditivity the entropy loss in D_0 is at least

$$\sum_{\{i,j\} \in C'} (1 - \mathbf{H}_{x \sim D_0} [x_i \oplus x_j]) \geq |C'| \cdot (1 - \mathbf{H}[\beta(2/3)]) > \frac{\sqrt{(m - 1)\delta}}{18},$$

where $\beta(2/3)$ denotes the Bernoulli distribution with success probability $2/3$. Therefore,

$$\mathbf{H}_{D_0} [x] < m - \frac{\sqrt{(m - 1)\delta}}{18} = m - \sigma(m),$$

which is a contradiction.

The claim follows. ■ *Claim 4*

4.2 Analyzing $HMP_m^{(k)}$

Using k parallel copies of the protocol described in Section 4.1, we obtain a protocol for exact solution of $HMP_m^{(k)}$. The complexity of the new protocol is $O(k \log(m))$ and it uses $k \log(m)$ EPR pairs.

Now we apply Theorem 3 together with Claim 4 (note that $|Z_m| = m$ in the case of HMP_m). It follows that

Claim 5. *Any 1-way protocol of communication cost $o\left(\frac{k\sqrt{m}}{\log m}\right)$ correctly solves $HMP_m^{(k)}$ with probability $1/2^{\Omega\left(\frac{k}{\log m}\right)}$.*

4.2.1 Solving $HMP_m^{(k)}$ with limited entanglement

In this section we will abuse notation by not distinguishing between a *quantum state* and the corresponding density matrix.

The idea of our next argument is the following. Let C be a 1-way protocol of cost $o\left(\frac{k\sqrt{m}}{\log m}\right)$ which start with some entangled state ρ of $e(m, k)$ qubits shared between Alice and Bob and solves $HMP_m^{(k)}$ with probability at least δ . Denote by τ the maximally mixed quantum state over $e(m, k)$ qubits. Consider a modification of the protocol C where instead of ρ we use τ , let us call this new protocol C' .

On the one hand, by the laws of quantum mechanics the success probability of C' must be at least $\delta/2^{e(m,k)}$. On the other hand, because the maximally mixed state over $e(m, k)$ qubits is not entangled, Claim 5 applies to C' . From that we will derive an upper bound on δ .

Let \tilde{C} be the measurement-free version of C (i.e., the communication channels are quantum and the output is a quantum state); similarly, let \tilde{C}' be the measurement-free version of C' . Denote by $U_{x,y}$ the unitary operator corresponding to the action of \tilde{C} on the shared entangled state when the inputs to Alice and Bob are x and y , correspondingly. In other words if the input pair is (x, y) then $U_{x,y}\rho U_{x,y}^\dagger$ and $U_{x,y}\tau U_{x,y}^\dagger$ are the quantum states obtained after running of \tilde{C} and \tilde{C}' , correspondingly.

Because τ is the maximally mixed state of dimension $2^{e(m,k)}$ therefore $\tau' = \frac{2^{e(m,k)}}{2^{e(m,k)}-1} \left(\tau - \frac{1}{2^{e(m,k)}} \right)$ is a quantum state too. We can express:

$$U_{x,y}\tau U_{x,y}^\dagger = \frac{2^{e(m,k)} - 1}{2^{e(m,k)}} \cdot U_{x,y}\tau' U_{x,y}^\dagger + \frac{1}{2^{e(m,k)}} \cdot U_{x,y}\rho U_{x,y}^\dagger.$$

Let us denote by $\Pi_{x,y}$ the projection of the final state of \tilde{C} to the subspace of correct answers to $HMP_m^{(k)}(x, y)$. Our assumption about C can be expressed as

$$\forall x, y \quad \text{tr}(\Pi_{x,y} U_{x,y} \rho U_{x,y}^\dagger) \geq \delta.$$

The success probability of \tilde{C}' is

$$\text{tr}(\Pi_{x,y} U_{x,y} \tau U_{x,y}^\dagger) \geq \frac{1}{2^{e(m,k)}} \cdot \text{tr}(\Pi_{x,y} U_{x,y} \rho U_{x,y}^\dagger) \geq \frac{\delta}{2^{e(m,k)}}.$$

As mentioned above, Claim 5 applies to C' and therefore for m sufficiently large, $\frac{\delta}{2^{e(m,k)}} \in 2^{-\Omega\left(\frac{k}{\log m}\right)}$. Therefore, the protocol C can be successful with constant probability only if $e(m, k) \in \Omega(k)$. This concludes our complexity analysis for $HMP_m^{(k)}$.

Claim 6. *In the SMP model, $HMP_m^{(k)}$ can be solved exactly by a protocol of cost $O(k \log(m))$ using $k \log(m)$ shared EPR pairs.*

In the 1-way communication model with any shared entangled state of $o\left(\frac{k}{\log m}\right)$ qubits, the communication cost of solving $HMP_m^{(k)}$ with constant-bounded error is $\Omega\left(\frac{k\sqrt{m}}{\log m}\right)$.

Theorem 1 follows from this claim.

5 Connection to 2-prover proof systems

Consider the following argument. Starting with the known 2-prover classical proof system which accepts $NEXP$, let us improve its soundness by sequentially repeating the protocol polynomially-many times. We know that the same proof system is not valid if the provers share entanglement because they can cheat ([CHTW04]). However, a straightforward modification of our entanglement bounding approach shows that *in order to cheat, the provers require the number of entangled qubits asymptotically close to the number of repetitions.*

Therefore, if the number of shared entangled qubits is bounded by some a priori fixed polynomial in the input length, we can introduce enough repetitions to make any cheating impossible (cf. Subsection 4.2.1). In combination with the result of [KM03], this leads to the following conclusion.

Claim 7. *Let $MIP_{e(n)}^*$ be the model of 2-prover proof systems in which the provers are allowed to share any entangled state over $e(n)$ qubits, where n is the input length. If $e(n) \in \text{poly}(n)$ then $MIP_{e(n)}^*$ can accept a language L if and only if $L \in NEXP$.*

In other words, the power of $MIP_{e(n)}^*$ is the same as that of the classical 2-prover proof systems, which is equivalent to $NEXP$.

6 Discussion

In this paper we solve one of the open question regarding the power of quantum entanglement in communication complexity: we show that no general sublinear upper bound on the required amount of shared entanglement can be put in the models of classical communication with either 1-way or simultaneous message passing. Can similar results be obtained for other communication models?

In Section 5 we showed a simple modification of our entanglement bounding ideas which leads to some nontrivial statement regarding the power of 2-prover proof systems with shared entanglement. Can we find other applications of our technique outside the domain of communication complexity? Possible applications to other communication complexity models might be interesting too. Given that the power of entanglement is one of the most important longstanding open problems in the area, it is very tempting to look for other applications of our technique.

There are some more technical questions. Can we find more uses for our strong direct product theorem for relations? It would be interesting to find applications other than *HMP*, though even with that relation it might probably lead to more results in communication complexity. The importance of *HMP* stems from the fact that this is the only problem we know today which demonstrates superpolynomial (in fact, exponential) separation between quantum and classical 1-way communication models.

It would be also interesting to see whether results similar to ours can be demonstrated through functional problems, either total or partial (the latter means that some combinations of (x, y) can never appear in the input).

The last question we would like to mention is whether independent EPR pairs provide a universal source of entanglement in the contexts of 2-party communication complexity and 2-prover proof systems.

Acknowledgments

I thank John Watrous and Ronald de Wolf for helpful discussions.

References

- [A04] S. Aaronson. Limitations of Quantum Advice and One-Way Communication. *Proceedings of the 19th IEEE Conference on Computational Complexity*, pp. 320-332, 2004.
- [B] H. Buhrman - *Personal communication*.
- [BFL90] L. Babai, L. Fortnow and C. Lund. Non-Deterministic Exponential Time Has Two-Prover Interactive Protocols. *Proceedings of the 31st Annual Symposium on Foundations of Computer Science*, pp. 16-25, 1990.
- [BJK04] Z. Bar-Yossef, T. S. Jayram and I. Kerenidis. Exponential separation of quantum and classical one-way communication complexity. *Proceedings of 36th Symposium on Theory of Computing*, pp. 128-137, 2004.
- [CHTW04] R. Cleve, P. Høyer, B. Toner and J. Watrous. Consequences and limits of nonlocal strategies. *Proceedings of the 19th IEEE Conference on Computational Complexity*, pp. 236-249, 2004.

- [GKRW06] D. Gavinsky, J. Kempe, O. Regev and R. de Wolf. Bounded-error Quantum State Identification and Exponential Separations in Communication Complexity. *Proceedings of the 38th Symposium on Theory of Computing*, 2006.
- [GS86] S. Goldwasser and M. Sipser. Private Coins versus Public Coins in Interactive Proof Systems. *Proceedings of the 18th Symposium on Theory of Computing*, pp. 59-86, 1986.
- [JRS05] R. Jain, J. Radhakrishnan and P. Sen. Prior Entanglement, Message Compression and Privacy in Quantum Communication. *Proceedings of the 20th IEEE Conference on Computational Complexity*, pp. 285-296, 2005.
- [KM03] H. Kobayashi and K. Matsumoto. Quantum Multi-prover Interactive Proof Systems with Limited Prior Entanglement. *Journal of Computer and System Sciences* 66(3), pp. 429-450, 2003.
- [KSW04] H. Klauck, R. Spalek and R. de Wolf. Quantum and Classical Strong Direct Product Theorems and Optimal Time-Space Tradeoffs. *Proceedings of the 45th Annual Symposium on Foundations of Computer Science*, pp. 12-21, 2004.
- [N91] I. Newman. Private vs. Common Random Bits in Communication Complexity. *Information Processing Letters* 39(2), pp. 67-71, 1991.
- [NS96] I. Newman and M. Szegedy. Public vs. Private Coin Flips in One Round Communication Games. *Proceedings of the 28th Symposium on Theory of Computing*, pp. 561-570, 1996.
- [R95] R. Raz. A parallel repetition theorem. *Proceedings of the 27th Symposium on Theory of Computing*, pp. 447-456, 1995.
- [S05] Y. Shi. Tensor norms and the classical communication complexity of bipartite quantum measurements. *Proceedings of the 37th Symposium on Theory of Computing*, 2005.